Des. Codes Cryptogr. (2008) 48:287–292
DOI 10.1007/s10623-008-9207-5

On orthogonal resolutions of the classical Steiner quadruple system SQS(16)

Hans Ludwig de Vries

Received: 22 February 2008 / Revised: 20 March 2008 / Accepted: 25 March 2008 /
Published online: 16 April 2008

Abstract A *Steiner quadruple system* SQS(16) is a pair $(V, \mathcal{B})$ where V is a 16-set of *objects* and $\mathcal{B}$ is a collection of 4-subsets of V, called *blocks*, so that every 3-subset of V is contained in exactly one block. By *classical* is meant the *boolean* quadruple system, also known as the affine geometry AG(4,2). A *parallel class* is a collection of four blocks which partition V. The system possesses a *resolution* or *parallelism*, since $\mathcal{B}$ can be partitioned into 35 parallel classes. Two resolutions are called *orthogonal* when each parallel class of one resolution has at most one block in common with each parallel class of the other resolution. We prove that there are at most nine further resolutions which, together with the classical one, are pairwise orthogonal.

Keywords Steiner quadruple system · Automorphism group · Resolutions

AMS Classifications 05B05 · 05B07 · 51E10

1 The automorphism group M of the SQS(16)

The Reverend T. P. Kirkman knew in 1862 that there exists a group of degree 16 and order 322560 with a normal, elementary abelian, subgroup of order 16 [1, p. 108]. Frobenius identified this group in 1904 as a subgroup of the Mathieu group M_{24} [4, p. 570]:

$\mathfrak{M}_{16}$ ist die dreifach transitive lineare Gruppe der Ordnung

$$2^4(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3).$$

Communicated by J. D. Key.

H. L. de Vries (✉)
Institut für Numerische und Angewandte Mathematik, Georg-August-Universität Göttingen,
Lotzestraße 16-18, 37083 Göttingen, Germany
e-mail: devries@math.uni-goettingen.de

Sie enthält die elementare Gruppe $\mathfrak{N}$ der Ordnung 16 als invariante Untergruppe, und $\dfrac{\mathfrak{M}_{16}}{\mathfrak{N}} = \mathfrak{T}_8$ ist der alternierenden Gruppe des Grades 8 isomorph.

In the ATLAS [3, p. 96] the group is noted as maximal subgroup of M_{24} with structure $2^4: A_8$. We call this group M with N its normal subgroup and generate $M := \langle\alpha, \gamma\rangle$ by

$$\alpha := (\mathtt{12498AE7F5BC36D}), \quad \gamma := (\mathtt{08})(\mathtt{1E2B5F496A3D7C}).$$

Then N consists of the identity and a conjugacy class of size 15,

$$N = (1) \cup \{\alpha^{-i}\gamma^7\alpha^i \mid i = 1, \ldots, F\}.$$

2 The SQS(16) and the orbits $\mathcal{O}_i$ of parallel classes

In 1980 Hartman [5] has given some sets of mutually orthogonal resolutions of quadruple systems, using groups $PSL(2, q)$. Hartman and Phelps [6] have raised the general resolvability question for SQS and stated: 'There is no good upper bound on the number of mutually orthogonal resolutions of an SQS (p. 226) ....'. We treat the special case of the SQS(16) where

$$V := \mathtt{0123456789ABCDEF}, \quad \mathcal{B} := \{\, gB \mid g \in M\}$$

with block $B := \mathtt{0123}$.

To form resolutions we need the set of parallel classes. A backtrack search reveals that its cardinality is $1505 = 43 \times 35$. The group M partitions it into orbits $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_3$ of lengths 35, 18×35 and 24×35. Orbit $\mathcal{O}_1$ is the SQS(16) which is listed explicitly in Appendix $\mathcal{O}_1$. The group M generates the orbits $\mathcal{O}_i = \{\, g\mathcal{P}_i \mid g \in M\}$ where the parallel classes are

	Block numbers				Parallel classes			
$\mathcal{P}_1$	1	102	127	140	0123	4567	89AB	CDEF
$\mathcal{P}_2$	1	102	128	139	0123	4567	89CD	ABEF
$\mathcal{P}_3$	1	103	125	139	0123	4589	67CD	ABEF

The four blocks of every parallel class $\mathcal{P} \in \mathcal{O}_2$ lie in *two* parallel classes of $\mathcal{O}_1$: *No* resolution in $\mathcal{O}_2$ is orthogonal to $\mathcal{O}_1$.

The four blocks of every parallel class $\mathcal{P} \in \mathcal{O}_3$ lie in *four* parallel classes of $\mathcal{O}_1$: *Every* resolution in $\mathcal{O}_3$ is orthogonal to $\mathcal{O}_1$.

3 The normal subgroup N and its subgroups

The non-identity elements of N consist of eight 2-cycles (i, j), $0 \le i < j \le F$, which we call δ_j if the first 2-cycle is $(0, j)$. Altogether their number is $15 \times 8 = \binom{16}{2}$. They are listed in Appendix N. They describe a 'proper edge coloring' of the complete graph K_{16}.

The group N and its subgroups lead to a Steiner triple system and its subsystems. A Steiner triple system STS(v) is a collection of blocks of size 3 taken from a v-set of objects such that every two objects belong to precisely one block. Since N is the direct product of four groups of order 2 we create an STS(15) by taking as objects the 15 permutations $\delta_i \in N$ and as blocks the triples $\{\delta_i, \delta_j, \delta_i\delta_j\}$. It is isomorphic to the *derivation* of the SQS(16) of

Appendix $\mathcal{O}_1$: Take there the first 35 blocks, delete the object 0, and an STS(15) is left over. Its objects i are the δ_i here. The systems are isomorphic to the STS(15) of [7, p. 17] and [2, p. 65 #1].

The automorphism group of the STS(15) is the $PSL(4,2)$ of order 20160. It is generated by

$$\alpha := (\texttt{12498AE7F5BC36D}), \quad \beta := (\texttt{1254637})(\texttt{9ADCEBF}),$$

taken over from [7, p. 17]. The permutation β has in M the *unique* square root γ, $\gamma^2 = \beta$. It is the reason we generate M by α and γ. Uniqueness of γ follows from the observation that in M the four conjugacy classes with representatives $\beta,\ \beta^{-1}$ of order 7 and $\gamma,\ \gamma^{-1}$ of order 14 have the *same* size 23040.

4 Partitioning $\mathcal{O}_3$ into 15 tiles $\mathcal{T}_i$

Let N act on each parallel class $\mathcal{P} \in \mathcal{O}_3$: The stabilizers $Stab_N(\mathcal{P})$ are of order 2, so every $\mathcal{P} \in \mathcal{O}_3$ is fixed by a unique $\delta_i \in N$. They partition $\mathcal{O}_3$ into 15 sets of parallel classes which we call *tiles* $\mathcal{T}_i$,

$$\mathcal{T}_i := \{\mathcal{P} \in \mathcal{O}_3 \mid \delta_i \mathcal{P} = \mathcal{P}\}.$$

The tiles are of cardinality $(24 \times 35)/15 = 56$, involved are 28 blocks of multiplicity 8. The permutation $\alpha \in M$ of order 15 permutes the tiles. Incidentally, the 140 blocks $B \in \mathcal{B}$ have stabilizers $Stab_N(B)$ of order 4. In the following proposition we use the definition of orthogonal resolutions [6, pp. 225–226] also for pairs of sets of parallel classes.

5 Two propositions and the theorem

Proposition 1 *The* 15 *tiles* $\mathcal{T}_i$ *are pairwise orthogonal.*

Proof If a parallel class $\mathcal{P}$ is sent to $\mathcal{T}_i$, it takes with it all the $\binom{4}{2} = 6$ parallel classes which have two blocks with $\mathcal{P}$ in common. For example, as the parallel class $\mathcal{P}_3 \in \mathcal{O}_3$ goes to $\mathcal{T}_1$, so do the six others:

1	103	125	139	0123	4589	67CD	ABEF
1	103	126	138	0123	4589	67EF	ABCD
1	104	125	129	0123	45AB	67CD	89EF
1	105	123	139	0123	45CD	6789	ABEF
7	67	103	125	01EF	23AB	4589	67CD
3	68	103	139	0167	23CD	4589	ABEF
4	64	125	139	0189	2345	67CD	ABEF

The reason: Pairs of $\delta_1 = (\texttt{01})(\texttt{23})(\texttt{45})(\texttt{67})(\texttt{89})(\texttt{AB})(\texttt{CD})(\texttt{EF})$ are pairs in the blocks.

This set of seven parallel classes can be called a ‘sphere’, the first one being its ‘centre’. A tile can in 105 ways be covered with a perfect ‘sphere packing’ of eight spheres, $8 \times 7 = 56$. □

Proposition 2 *In every tile the maximal number of its* 56 *parallel classes which have pairwise at most one block in common is equal to* 21.

Proof By backtrack searches. In a tile there are eight such 21-sets. They consist of all the 28 blocks of its tile, each block appearing three times. □

From the two propositions follows the result of this paper:

Theorem *The classical SQS*(16) *has at most* 9 *more resolutions such that they are pairwise orthogonal.*

Proof

$$15 \times 21 = 9 \times 35.$$

□

6 A lower bound

Here is an example of six pairwise orthogonal resolutions in $\mathcal{O}_3$. Provided $\mathcal{O}_3$ is sorted we represent its parallel classes by *positional parameters*. The 24 letters $a, \ldots, x$ stand for the numbers $1, \ldots, 24$. A letter z at position s, $1 \leq s \leq 35$, refers to the parallel class $\mathcal{P}_j$ where $j = (s-1) \times 24 + z$. A first resolution is

`amgtxdumchdunuqmeqhebqkhpxxmnbiwdto.`

To produce four more let the group $\langle \alpha^3 \rangle$ act on it. Their automorphism groups are the identity. The sixth resolution with automorphism group $\langle \alpha^3 \rangle$ is

`jbjumtiuxeaxkptluidlgjmfbqidfdtqumv.`

Earlier Hartman [5, p. 162] has given a set of seven mutually orthogonal resolutions of an SQS$(q+1)$ for $q = 43$.

7 Orbit $\mathcal{O}_2$

Every parallel class $\mathcal{P} \in \mathcal{O}_2$ has a stabilizer $Stab_N(\mathcal{P})$ of order 8. For the $\mathcal{P}_2 \in \mathcal{O}_2$ it is the subgroup N' of N,

$$N' := (1) \; \cup \; \{\delta_i \in N \mid i = 1, \ldots, 7\}.$$

There are 15 stabilizers, the conjugacy class $\{\alpha^{-i} N' \alpha^i \mid i = 1, \ldots, F\}$. They partition $\mathcal{O}_2$ into 15 sets of cardinality $(18 \times 35)/15 = 42$ which are not pairwise orthogonal. The stabilizers lead to the 15 subsystems (Fano planes) STS(7) of the STS(15) [7, p. 17].

Acknowledgments The author thanks Eberhard Schmitt for helpful discussions and the Institut für Numerische und Angewandte Mathematik at Göttingen for generous hospitality.

Appendices

Appendix N The normal subgroup N, elements $\neq (1)$

$\delta_1 :=$ `(01)(23)(45)(67)(89)(AB)(CD)(EF)`
$\delta_2 :=$ `(02)(13)(46)(57)(8A)(9B)(CE)(DF)`

δ_3 := (03)(12)(47)(56)(8B)(9A)(CF)(DE)
δ_4 := (04)(15)(26)(37)(8C)(9D)(AE)(BF)
δ_5 := (05)(14)(27)(36)(8D)(9C)(AF)(BE)
δ_6 := (06)(17)(24)(35)(8E)(9F)(AC)(BD)
δ_7 := (07)(16)(25)(34)(8F)(9E)(AD)(BC)
δ_8 := (08)(19)(2A)(3B)(4C)(5D)(6E)(7F)
δ_9 := (09)(18)(2B)(3A)(4D)(5C)(6F)(7E)
δ_A := (0A)(1B)(28)(39)(4E)(5F)(6C)(7D)
δ_B := (0B)(1A)(29)(38)(4F)(5E)(6D)(7C)
δ_C := (0C)(1D)(2E)(3F)(48)(59)(6A)(7B)
δ_D := (0D)(1C)(2F)(3E)(49)(58)(6B)(7A)
δ_E := (0E)(1F)(2C)(3D)(4A)(5B)(68)(79)
δ_F := (0F)(1E)(2D)(3C)(4B)(5A)(69)(78)

Appendix $\mathcal{O}_1$ The SQS(16)

Block numbers				Parallel classes			
1	102	127	140	0123	4567	89AB	CDEF
2	65	128	139	0145	2367	89CD	ABEF
3	64	129	138	0167	2345	89EF	ABCD
4	67	105	126	0189	23AB	45CD	67EF
5	66	106	125	01AB	2389	45EF	67CD
6	69	103	124	01CD	23EF	4589	67AB
7	68	104	123	01EF	23CD	45AB	6789
8	43	130	137	0246	1357	8ACE	9BDF
9	42	131	136	0257	1346	8ADF	9BCE
10	45	109	122	028A	139B	46CE	57DF
11	44	110	121	029B	138A	46DF	57CE
12	47	107	120	02CE	13DF	468A	579B
13	46	108	119	02DF	13CE	469B	578A
14	37	132	135	0347	1256	8BCF	9ADE
15	36	133	134	0356	1247	8BDE	9ACF
16	39	113	118	038B	129A	47CF	56DE
17	38	114	117	039A	128B	47DE	56CF
18	41	111	116	03CF	12DE	478B	569A
19	40	112	115	03DE	12CF	479A	568B
20	53	80	101	048C	159D	26AE	37BF
21	52	81	100	049D	158C	26BF	37AE
22	55	78	99	04AE	15BF	268C	379D
23	54	79	98	04BF	15AE	269D	378C
24	49	84	97	058D	149C	27AF	36BE
25	48	85	96	059C	148D	27BE	36AF
26	51	82	95	05AF	14BE	278D	369C
27	50	83	94	05BE	14AF	279C	368D
28	61	72	93	068E	179F	24AC	35BD
29	60	73	92	069F	178E	24BD	35AC
30	63	70	91	06AC	17BD	248E	359F
31	62	71	90	06BD	17AC	249F	358E
32	57	76	89	078F	169E	25AD	34BC
33	56	77	88	079E	168F	25BC	34AD
34	59	74	87	07AD	16BC	258F	349E
35	58	75	86	07BC	16AD	259E	348F

References

1. Biggs N.L., T. P. Kirkman.: Mathematician Bull. London Math. Soc. **13**, 97–120 (1981).
2. Colbourn C.J., Rosa A.: Triple Systems. Clarendon Press, Oxford (1999).
3. Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson R.A.: Atlas of Finite Groups. Oxford University Press, Oxford (1985).
4. Frobenius G.: Über die Charaktere der mehrfach transitiven Gruppen. Sitzungsber. Königl. Preuss. Akad. Wiss. Berlin, 558–571 (1904). Reprinted in Serre J.-P. (ed.) Frobenius F.G., Abhandlungen G. III, pp. 335–348. Springer, Berlin (1968).
5. Hartman A.: Doubly and orthogonally resolvable quadruple systems. In: Robinson R.W., Southern G.W., Wallis W.D. (eds.) Combinatorial Mathematics VII, Lecture Notes in Mathematics, vol. 829, pp. 157–164. Springer, Berlin (1980).
6. Hartman A., Phelps K.T.: Steiner quadruple systems. In: Dinitz J.H., Stinson D.R. (eds.) Contemporary Design Theory: A Collection of Surveys, pp. 205–240. Wiley, New York (1992).
7. Mathon R.A., Phelps K.T., Rosa A.: Small Steiner triple systems and their properties. Ars Combin. **15**, 3–110 (1983).